

Tax Season, Open Season: Phishing and Malware Campaigns Targeting Indian Taxpayers

 cloudsek.com/blog/tax-season-open-season-phishing-and-malware-campaigns-targeting-indian-taxpayers

Shobhit Mishra

July 30, 2026

Executive Summary

Every year the ITR filing window turns into a hunting ground. Taxpayers are already thinking about deadlines, refunds, and penalty notices, so a message that mentions any of those three lands on fertile soil. Attackers know this, and they time their operations to match it.

This advisory breaks down a live campaign our team reviewed, built from scam samples that victims posted on X and from phishing infrastructure we analysed directly. The lure is a fake Income Tax Department penalty notice delivered over WhatsApp and messaging apps. The payload is a ZIP file that drops malware. Around it sits a wider ecosystem of refund SMS fraud, cloned e-Filing portals, fake e-PAN emails, and refund agents who are really just data harvesters.

The single most important fact to carry into this season: the Income Tax Department does not serve statutory notices, penalty orders, or summons over WhatsApp. Any tax notice that arrives as a WhatsApp file from an unknown number is fraudulent, full stop.

Key findings

- A fake Office Memorandum citing Section 271(1)(c) and Section 276C of the Income Tax Act, 1961 is being pushed to taxpayers over WhatsApp and other chat apps by unknown or compromised accounts.
- The notice is bilingual (Hindi and English), carries the Government of India emblem, a fake reference number, and a spoofed signatory (“Raj Kumar Sharma, Assistant Commissioner of Income Tax”). It demands action within 72 hours.
- The “Download Documents” button on the linked page fetches an ITD.zip archive that contains malicious binaries, not documents.
- The ZIP is served in multiple sizes (observed at 2 MB, 34 MB, and 35 MB across samples), which points to payload rotation, a common way to stay ahead of static signature detection.
- The phishing pages sit on throwaway domains using cheap, low-trust TLDs (.lol, .xin, .ink, .autos). None of them are incometax.gov.in.

- This activity overlaps with campaigns tracked publicly through 2026 that deliver remote access trojans and infostealers under income tax lures, so treat any infection as credential theft and remote access, not a nuisance file.

Why the timing matters

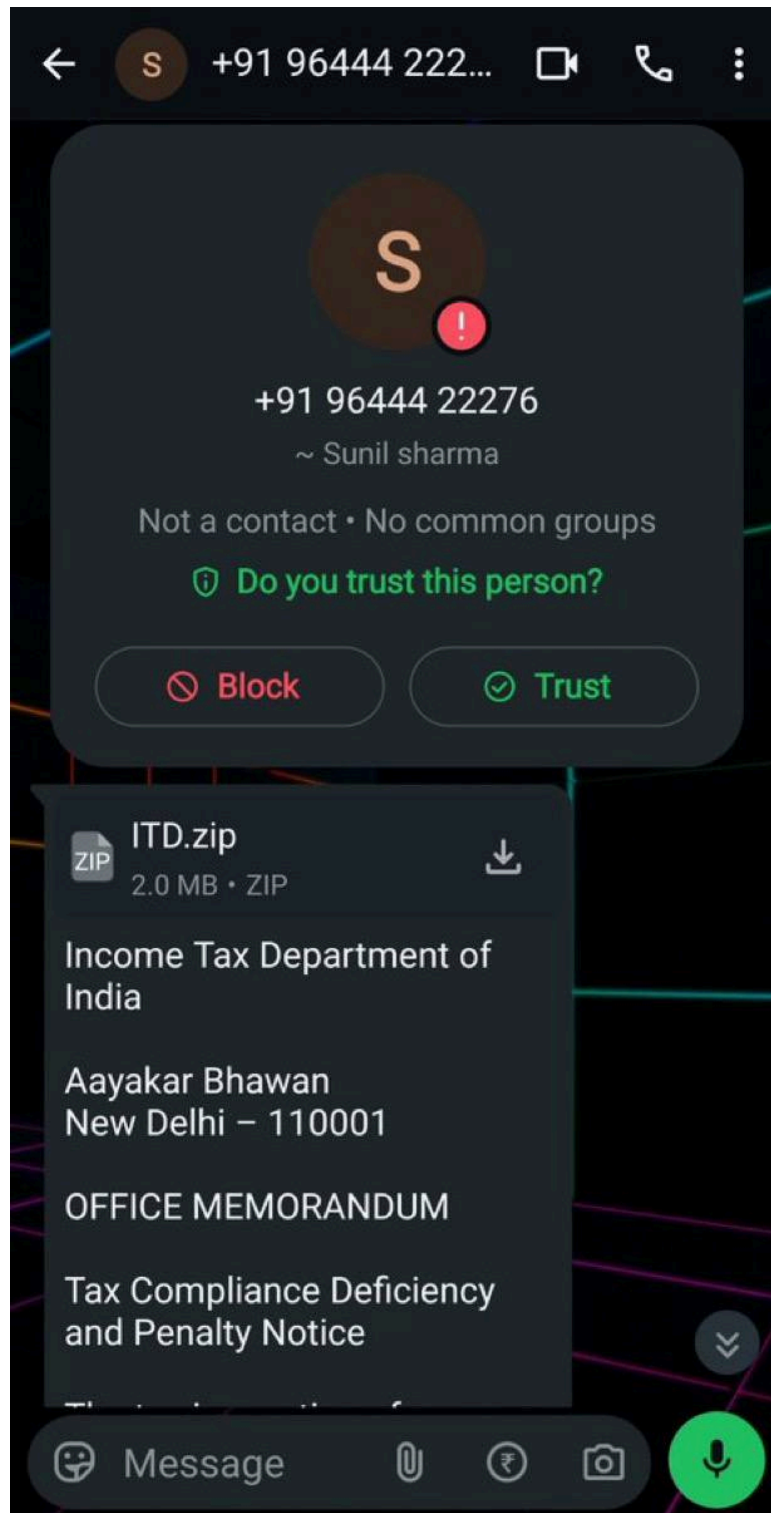
Tax-themed phishing and malware surge during and just after ITR season. With public conversation focused on refund timelines and last dates, a fake notice or a fake refund-pending message reads as plausible because it matches what people are already expecting to receive. Security researchers analysing this year's income tax lures describe the operations as deliberate and sustained rather than opportunistic, citing precise lure documents, real legal citations, bilingual content, and active payload rotation as evidence of a resourced effort focused on Indian taxpayers.

The emotional engine is simple. A refund message sells hope. A penalty notice sells fear. Both push you to act before you think, which is exactly the state an attacker wants you in.

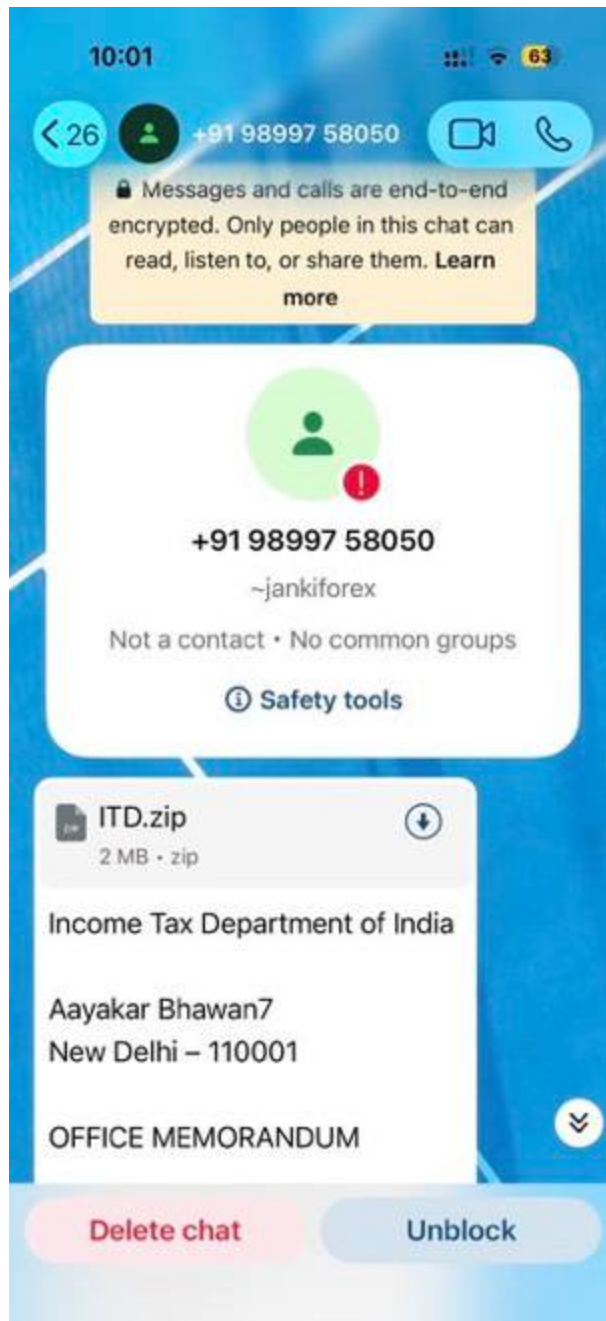
Anatomy of the WhatsApp penalty-notice campaign

How it reaches you

This threat is delivered entirely inside the chat. There is no website and no link. An unknown number sends a file directly on WhatsApp or a similar app, along with a block of official-sounding text that begins "Income Tax Department of India, Aayakar Bhawan, New Delhi 110001, OFFICE MEMORANDUM." In the samples reviewed, the sender profiles had nothing to do with tax administration: display names such as "Sunil sharma", "jankiforex", and "Hotel Oyster", each flagged by the app as Not a contact. One sample was pushed inside a group chat. These are almost certainly random or compromised accounts being used to spread the file.



Unknown number posing as "Sunil sharma" delivering ITD.zip

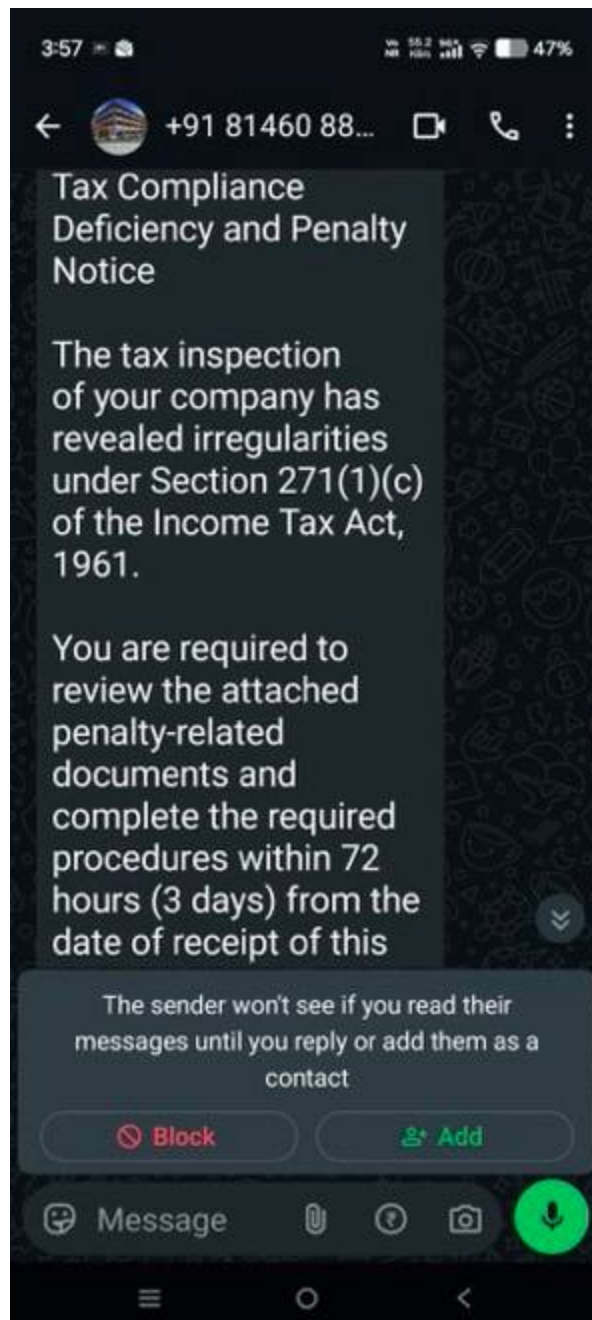


Another unknown sender (“jankiforex”) with the same ITD.zip lure.

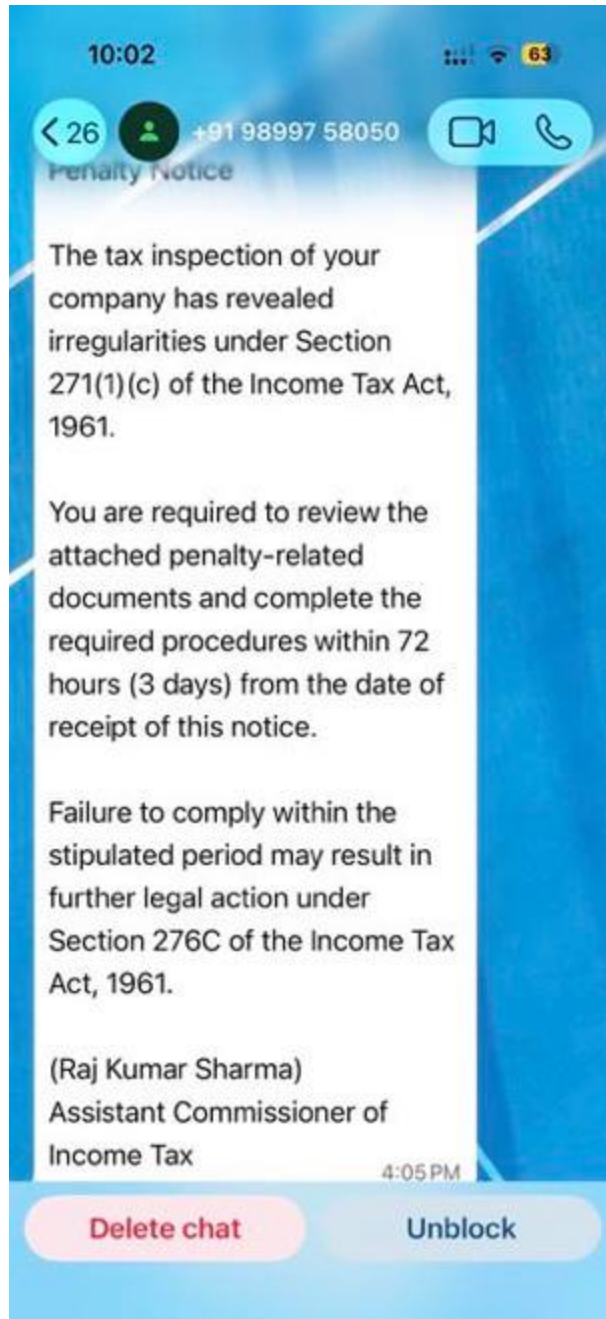
What the file actually is

The attachment is presented as ITD.zip, but the payload is a malicious Android application (APK). It is not a document and it is not a genuine utility. Installing it on an Android phone is the whole objective. Once installed, malware of this kind typically requests broad permissions and can read and intercept SMS (including one-time passwords used by banks), harvest contacts to spread the file further, capture keystrokes, and overlay fake screens on top of banking and payment apps to steal credentials. The differing file sizes seen across samples

(2 MB versus 34 to 35 MB) point to different builds or payload rotation, a common way to stay ahead of static detection.



The message text: Section 271(1)(c), a 72-hour deadline, and a Section 276C threat.



The same script reused verbatim across different sender accounts.

What to do: never install an APK sent to you in a chat, no matter who it claims to be from. The Income Tax Department does not send apps or notices over WhatsApp. Delete the message, and do not tap the file.

Fake Income Tax websites (new and emerging)

The setup

This is a separate operation that lives on the web rather than in a chat. Attackers are standing up a wave of newly registered lookalike domains that impersonate the Income Tax Department. Victims are steered to these pages through emails, messages, or search, and the page is built to look like an official government notice. The infrastructure is disposable by design, so the specific domains rotate quickly.

The lure page

Each site hosts a forged Office Memorandum. It is a competent fake. It reproduces the Government of India emblem and an Income Tax Department, Ministry of Finance header; a fabricated file number (for example, No. TAX/PEN/2026-142) and the Aayakar Bhawan address; bilingual Hindi and English body text, which makes it feel institutional; a specific legal hook, the claim of irregularities under Section 271(1)(c) with a threat of action under Section 276C; a hard 72-hour deadline; and a spoofed signatory, Raj Kumar Sharma, Assistant Commissioner of Income Tax.



Income Tax Department Ministry of Finance, Government of India

No. TAX/PEN/2026-142

भारत सरकार / Government of India

वित्त मंत्रालय / Ministry of Finance
आयकर विभाग / Income Tax Department
प्रवर्तन प्रभाग / Enforcement Division

Aayakar Bhawan,
New Delhi - 110001

OFFICE MEMORANDUM

Sub: कर अनुपालन की कमी और दंड सूचना / Tax Compliance Deficiency and Penalty Notice

- आपकी कंपनी की कर निरीक्षण के दौरान आयकर अधिनियम, 1961 की धारा 271(1)(c) के तहत कर संबंधी अनियमितताएं पाई गई हैं। The tax inspection of your company has revealed irregularities under Section 271(1)(c) of the Income Tax Act, 1961.
- इस सूचना की प्राप्ति के 72 घंटे (3 दिन) के भीतर निम्नलिखित दस्तावेज़ आयकर विभाग को प्रस्तुत करना अनिवार्य है। It is mandatory to submit the following documents to the Income Tax Department within 72 hours (3 days) of receipt of this notice.

आवश्यक दस्तावेज़ सूची / Required Documents List

नीचे दिए गए लिंक से दस्तावेज़ डाउनलोड करें / Download documents from the link below

 दस्तावेज़ डाउनलोड करें / Download Documents

- निर्धारित समयावधि में दस्तावेज़ प्रस्तुत न करने पर आयकर अधिनियम की धारा 276C के तहत कानूनी कार्रवाई की जाएगी। Legal action will be taken under Section 276C of the Income Tax Act if documents are not submitted within the stipulated time.

The forged Office Memorandum hosted on the fake sites (footer confirms the host domain). Everything above the button exists to justify the button.

The payload

The only functional element on the page is a “Download Documents” button. It does not fetch documents. It downloads malware binaries onto the visitor's computer. Campaigns using this

exact playbook this year have chained an archive or disk image to a signed-binary sideload, then loaded a remote access trojan or an infostealer into memory. The practical impact is remote control of the machine and theft of credentials, browser data, and financial information.

The infrastructure

The pages are hosted on disposable domains built to be discarded and replaced. Defanged for safety, the infrastructure we reviewed is listed below.

Indicator	Type	Notes
apeal[.]lol	Domain	Hosts the fake Office Memorandum. "Download Documents" delivers malware binaries.
ITD.zip	Filename	Malicious archive. Served at rotating sizes (2 MB / 34 MB / 35 MB observed).
22[.]laoshunfa[.]xyz	Domain	Same fake notice and payload flow.
audet[.]club	Domain	Same fake notice and payload flow.
bcgovtop[.]lol	Domain	Same fake notice and payload flow.
ckoming[.]study	Domain	Same fake notice and payload flow.
clerk[.]lat	Domain	Same fake notice and payload flow.
fsyahsxd[.]xin	Domain	Same fake notice and payload flow.
gisudyawz[.]ink	Domain	Same fake notice and payload flow.
gova[.]bar	Domain	Same fake notice and payload flow.
gova[.]lat/1.html	Domain	Same fake notice and payload flow.
govj[.]one/index.html	Domain	Same fake notice and payload flow.
gov-xnui[.]com	Domain	Same fake notice and payload flow.
govtocki[.]shop	Domain	Same fake notice and payload flow.
ingovtop[.]click	Domain	Same fake notice and payload flow.

Indicator	Type	Notes
kcsueaw[.]xin	Domain	Same fake notice and payload flow.
konimqh[.]study	Domain	Same fake notice and payload flow.
laiuatexqw[.]cc	Domain	Same fake notice and payload flow.
laoshunfa[.]xyz	Domain	Same fake notice and payload flow.
lzaiwugsa[.]ink	Domain	Same fake notice and payload flow.
oder[.]autos	Domain	Same fake notice and payload flow.
qaksdiuw[.]xin	Domain	Same fake notice and payload flow.
sfinmgov[.]club	Domain	Same fake notice and payload flow.
tarif[.]lol	Domain	Same fake notice and payload flow.
tzawccsw[.]xin	Domain	Same fake notice and payload flow.
xcvgyuraw[.]live	Domain	Same fake notice and payload flow.
zixhasda[.]xin	Domain	Same fake notice and payload flow.
zuytyarws[.]xin	Domain	Same fake notice and payload flow.
zxizusuy[.]xin	Domain	Same fake notice and payload flow.
zasudtytw[.]xin	Domain	Same fake notice and payload flow.
zytsyxbwa[.]live	Domain	Same fake notice and payload flow.
indiaaba[.]com	Domain	Same fake notice and payload flow.

The pattern is worth internalising, because the specific domains will be dead within days. Random consonant strings on cheap TLDs, no relationship to any government namespace, and a single call to action to download a file. That shape is the signature, more durable than any one URL.

Under the hood: the Windows payload (ITD_Tax_Notice.exe)

Desktop victims, including anyone who opens the archive from WhatsApp Web, receive a Windows executable named ITD_Tax_Notice.exe. We detonated the sample in the Sandbox. The verdict was malicious.

Indicators of compromise: ITD_Tax_Notice.exe

File and signing indicators:

Field	Value
Filename	ITD_Tax_Notice.exe
File type / size	PE32 executable (GUI), Intel 80386; 3,265,096 bytes
MD5	dff2b7a23882445b4e354199bf38554f
SHA-1	7479fbc27320ae246db9030cca80809ec63de0e9
SHA-256	667b37eafb9ec5131ed4f017ed429a47dca3adf626b2fc85fc6424b1e17ff6e1
Import hash	538ad8e0ad1fec0ecc54f9e120ac6ff9
Signing CA	Certum Extended Validation Code Signing 2021 CA
Signer (subject)	Chinese sole proprietor, Linyi, Shandong, CN (masquerades as a Microsoft svchost binary)
Cert serial	2D85A7A16D1EB86DFD92B00F6267733D

Network indicators (defanged):

Indicator	Type	Notes
vss2.oss-cn-hongkong[.]aliyuncs[.]com	Staging host	Alibaba Cloud OSS bucket (Hong Kong), 47.79.66.58. Abused to host the second stage.

Indicator	Type	Notes
hxxps://vss2.oss-cn-hongkong[.]aliyuncs[.]com/88.bin	2nd-stage payload	Follow-on binary fetched after execution.

All indicators are defanged. Do not visit these URLs directly.

The first stage is small, packed, and disguised as svchost.exe. Its job is to fingerprint the machine (the ipwho.is geolocation call) and then pull the real malware from the cloud. The second stage is delivered as a raw .bin : it is most likely shellcode or an encrypted blob that the loader decrypts and runs directly in memory, so the malicious code never lands on disk as a scannable executable. Hosting it in an Alibaba Cloud bucket also lets the operators swap the payload per victim, which fits the different archive sizes seen across the WhatsApp samples.

Key behaviours

- Masquerades as a Windows system process. The file's version metadata claims the original filename is svchost.exe, the description is Service Host, and the publisher is Microsoft Windows, while the company field reads only Windows Software Development Team. Dressing the binary up as svchost.exe helps it hide in plain sight.
- Packed and obfuscated. The file shows near-maximum entropy (about 8.0) and a writeable .text code section, both hallmarks of a runtime packer that unpacks malicious code in memory to defeat static scanning.
- Signed with an EV certificate to borrow trust. It carries a valid Certum Extended Validation code-signing certificate issued to a Chinese sole proprietor in Linyi, Shandong. A valid signature suppresses some warnings, and the mismatch between a Microsoft-looking svchost binary and a small sole-proprietor signer is itself a giveaway.
- Pulls a second stage from the cloud. On execution it reaches an Alibaba Cloud storage bucket in Hong Kong (vss2.oss-cn-hongkong[.]aliyuncs[.]com, 47.79.66.58) to fetch a follow-on payload named 88.bin. Hosting on a reputable cloud provider helps it slip past domain-reputation filters.
- Profiles the victim. It queries the legitimate geolocation service ipwho[.]is to determine the victim's IP location, useful for targeting and for filtering out analysis sandboxes.
- Evades analysis. The sandbox recorded modified sleep behaviour and virtualisation/sandbox checks, alongside registry, security-software, and system-information reconnaissance, before the process exited into Windows Error Reporting.

Only two network endpoints were observed, and both are legitimate services being abused: Alibaba Cloud storage for payload hosting and ipwho.is for geolocation. That is deliberate.

Traffic to well-known providers draws less attention than traffic to a freshly registered domain.

MITRE ATT&CK techniques observed

- Defense Evasion: Virtualization/Sandbox Evasion (T1497), DLL Side-Loading (T1574.002), Process Injection (T1055), Software Packing.
- Discovery: Query Registry (T1012), Security Software Discovery (T1518.001), System Network Configuration Discovery (T1016), System Information Discovery (T1082).
- Command and Control: Ingress Tool Transfer (T1105), Application Layer Protocol (T1071), Non-Application Layer Protocol (T1095), Encrypted Channel (T1573).

The wider tax-scam ecosystem this season

The penalty notice is one of several plays running in parallel. The others share the same psychology and the same goal.

Fake refund SMS, email, and WhatsApp messages

This is the volume play. A message claims a refund is pending, delayed, incomplete, or stuck, and demands urgent verification. It carries a link to a page that looks like the e-Filing site and asks for PAN, login credentials, OTP, and bank details. The Income Tax Department has publicly warned that these messages lean on alarming phrases like urgent action required, refund pending, or penalty if not verified, and it has stressed that it never asks for OTPs or bank details.

Refund Lure

Cloned e-Filing portals

Phishing sites replicate the look of the official Income Tax e-Filing portal, down to logos and layout, then harvest whatever you type: PAN, Aadhaar, password, OTP, bank account number. Stolen PAN alone is dangerous, because it can be used to open accounts, apply for loans, or launder money. The giveaway is almost always the address bar. Look-alike domains use slight misspellings or unrelated TLDs and never sit under [incometax.gov.in](https://www.incometax.gov.in).

Fake e-PAN and manual-verification

A recurring variant taxpayers a fake e-PAN file or asks them to manually verify attached documents to release a refund. India's PIB Fact Check unit has flagged these as fraudulent.

Red flags include generic greetings such as Hello Taxpayer or Dear User, a suspicious sender domain, and an unexpected attachment.

Fake SMS Lure

Fake tax consultants and refund agents

Not every scam is a link. Some are people. Fraudulent tax consultants and refund agents advertise fast or inflated refunds, then either collect fees and vanish, harvest your login and financial details, or file bogus deductions in your name that leave you exposed to a genuine notice later. If someone guarantees a refund figure before seeing your actual income and TDS data, that is a sales tactic, not tax advice.

Victim's Reddit Post

Red flags for taxpayers

Any one of these should stop you cold. Two together means walk away.

1. The message arrives on WhatsApp, SMS, or a chat app claiming to be a tax notice. Statutory notices, penalty proceedings, and summons are not served this way.
2. It comes from an unknown or personal mobile number, often with a display name that has nothing to do with the tax department.
3. It sets a short, aggressive deadline (72 hours, immediate action, final notice).
4. It asks you to download a file, especially a ZIP, or to click a button to download documents.
5. The link does not lead to incometax.gov.in. Treat .lol, .xin, .ink, .autos, and other odd TLDs, or misspelled look-alikes, as hostile by default.
6. It asks for your password, OTP, full bank details, or Aadhaar. The department never asks for these over email, SMS, or calls.
7. It uses a generic greeting (Dear Taxpayer, Dear User) rather than your name, or contains grammar and formatting that feels off.
8. A refund figure or a penalty is quoted before anyone has actually looked at your return.

Safety recommendations

For every taxpayer

- Treat any tax notice received over WhatsApp or SMS as fake. Do not open attachments and do not tap download buttons.

- Verify independently. Log in to the official e-Filing portal by typing the address yourself, and check whether any genuine notice exists. A real notice carries a Document Identification Number (DIN) that you can validate on the portal.
- Never share OTP, passwords, or full bank details in response to an inbound message, however official it looks.
- Bookmark the official portal and use only that bookmark. Never reach it through a link in a message.
- If you have already opened an ITD.zip or similar file, assume compromise. Disconnect the device from the network, change passwords from a different clean device (email and banking first), enable multi-factor authentication, run a full malware scan, and consult a qualified professional. Watch your bank and PAN-linked accounts closely.
- Report it. Forward suspicious tax communications to the department's reporting channel, and file cybercrime complaints through the national helpline (1930) or the official cybercrime portal.

For businesses and finance teams

- Run short awareness briefings during filing season. The people who receive compliance-notice emails are often in finance and HR, not IT.
- Block newly registered and low-trust TLDs at the gateway where feasible, and flag inbound archives and disk-image files for review.
- Route all tax filing and compliance through in-house experts or a verified, authorised professional, so that a random notice is easy to recognise as out of process.
- Watch for behavioural indicators of the malware families used in these campaigns: unusual svchost.exe paths, hidden system-folder directories, script engines running web-style files, and unexpected outbound connections.

References

*[Intelligence source and information reliability - Wikipedia](#)

#[Traffic Light Protocol - Wikipedi](#)



Shobhit Mishra



Jainam Shah

Cyber threat researcher focusing on tracking APT campaigns, OSINT and threat hunting.